

# Detection of Sinkhole attack in Wireless Sensor Networks using Mobile agent and multiple Base stations

Kripasinh Gohil

Affiliation: IT Dept., Shantilal Shah Engineering College, Gujarat

## ABSTRACT

A Wireless Sensor network (WSN) consists of large number of low power sensor nodes which are distributed in the wireless environment. Due to the wireless nature and infrastructure-less environment of WSN, they are more vulnerable to many types of security attacks. One of the most popular and serious attacks in wireless sensor networks is sinkhole attack. In Sinkhole attack, a compromised node advertises attractive and unfaithful routing information. It tries to get all traffic or high percentage of traffic from it. Sinkhole node can then launch more attacks, like selective forwarding, modifying or even dropping the packets coming through it. Several techniques are given in the literature. Most of these techniques use encryption-decryption mechanism which makes high overload to network. The proposed technique is to detect the sinkhole attack using multiple base stations and a mobile agent based technology. Multiple base stations ensure high packet delivery rate. Mobile agent is a software program which is self-controlling and it moves from node to node and checks the presence of sinkhole nodes in the network.

## General Terms

Wireless sensor network, Security, sinkhole attack, mobile agent, multiple basestations.

## Keywords

Wireless sensor network, sinkhole attack, mobile agent, multiple basestations.

## 1. INTRODUCTION

Rapid advances in the areas of sensor design, information technologies, and wireless networks have made the way for the creation of wireless sensor networks (WSN). Wireless Sensor Networks of hundreds of sensor nodes are already established and are being used. They are monitoring large geographic areas for different types of applications. The security is matter of concern in any type of network. Security is big concern for wireless sensor networks because of wireless and infrastructure-less nature. There are many mechanisms described in literature to manage security of wireless sensor networks.

Sensing is a technique used to gather information about a physical object or process, including the occurrence of events. An object performing such a sensing task is called a sensor. Which sensors should be chosen for an application depends on the physical property to be monitored, for

example, such properties include temperature, pressure, light, or humidity. When many sensors cooperatively monitor large physical environments, they form a Wireless Sensor Network [2].

Sensor nodes communicate not only with each other but also with a base station using their wireless radios, allowing them to spread their sensor data to remote processing, visualization, analysis, and storage systems [2]. Wireless sensor networks do not have pre-defined infrastructure. It contains devices with limited resources. The topology of wireless sensor network changes very frequently [3]. Wireless Sensor Network may have connection to Internet [2].

Sensor nodes consist of sensing, data processing, and communicating components. Sensor nodes are fitted with an on-board processor [3]. Sensor nodes may not have global identification (ID) because of the large amount of overhead and large number of sensors [3]. Instead of sending the raw data to the nodes responsible for the fusion, sensor nodes use their processing abilities to locally carry out simple computations and transmit only the required and partially processed data [3]. Sensor node architecture consists of following three components [2]:

- 1) *Sensing subsystem*: A physical sensor contains a transducer, a device that converts one form of energy into another form of energy, typically into an electrical energy. The output of this transducer is an analog signal having a continuous magnitude as a function of time. Therefore, an analog-to-digital converter is required to interface a sensing subsystem with a digital processor.
- 2) *Communication subsystem*: Its main purpose is to process (execute) instructions pertaining to sensing, communication, and self-organization. It consists of a processor chip, a non-volatile memory (usually an internal flash memory) for storing program instructions, an active memory for temporarily storing the sensed data, and an internal clock, among other things.

*Processor subsystem*: This subsystem is combination of Radio and coprocessor.

## 2. WSN APPLICATIONS

There are many types of sensor available. These sensors can monitor different conditions like temperature, humidity, vehicular movement, lightning condition, pressure, soil makeup, noise levels, the presence or absence of certain kinds of objects, mechanical stress levels on attached objects, and the current characteristics such as speed, direction, and size of an object [3]. The following are some applications of WSN [3]:

- 1) *Military applications:* Wireless sensor networks can be an integral part of military command, control, communications, computing, intelligence, surveillance, reconnaissance and targeting (C4ISR) systems.
- 2) *Environmental applications:* Some environmental applications of sensor networks include tracking the movements of birds, small animals, and insects; monitoring environmental; conditions that affect crops and livestock; irrigation; macro instruments for large-scale Earth monitoring and planetary exploration; chemical/ biological detection; precision agriculture; biological, Earth, and environmental monitoring in marine, soil, and atmospheric contexts; forest fire detection; meteorological or geophysical research; flood detection; bio-complexity mapping of the environment; and pollution study.
- 3) *Health applications:* Some of the health applications for sensor networks are providing interfaces for the disabled; integrated patient monitoring; diagnostics; drug administration in hospitals; monitoring the movements and internal processes of insects or other small animals; telemonitoring of human physiological data; and tracking and monitoring doctors and patients inside a hospital.
- 4) *Other applications:* There are some home applications such as home automation and smart environment. Some of the commercial applications are monitoring material fatigue; building virtual keyboards; managing inventory; monitoring product quality; constructing smart office spaces; environmental control in office buildings; robot control and guidance in automatic manufacturing environments; interactive toys; interactive museums; factory process control and automation; monitoring disaster area; smart structures with sensor nodes embedded inside; machine diagnosis; transportation; factory instrumentation; local control of actuators; detecting and monitoring car thefts; vehicle tracking and detection; and instrumentation of semiconductor processing chambers, rotating machinery, wind tunnels, and anechoic chambers.

## 3. WSN SECURITY RELATED ISSUES

The main objective of security is to achieve CIA security model. CIA stands for Confidentiality, Integrity, and Availability respectively. The Availability emerges as a top-priority security requirement [10]. In a WSN, successful packet delivery to the BS is more essentially required than the prevention of data to be captured by an attacker [6], [8], [9]. By using efficient data encryption algorithms such as AES and data anonymity techniques, the information

captured by an attacker can be made inconsequential. So, focus should be on the objective of delivering the packets to the BS [8].

### 3.1 Challenges and Limitations for security

The encryption-decryption techniques devised for the traditional wired networks are not feasible to be applied directly for the wireless networks and in particular for wireless sensor networks. WSNs consist of tiny sensors which really suffer from the lack of processing, memory and battery power. Applying any encryption scheme requires transmission of extra bits, hence extra processing, memory and battery power which are very important resources for the sensors' longevity. Applying the security mechanisms such as encryption could also increase delay, jitter and packet loss in wireless sensor networks. Moreover, some critical questions arise when applying encryption schemes to WSNs like, how the keys are generated or distributed. How the keys are managed, revoked, assigned to a new sensor added to the network or renewed for ensuring robust security for the network [13].

Cryptography provides a full range of cryptographic tools for authentication and protecting data against manipulations and unauthorized reading. The problem is that the classical methods are quite "heavy" and not well suited for sensor networks. The problems are communication overhead, computational resources necessary for performing cryptographic operations, key management and quite high probability of compromising some nodes [12].

Encryption and authentication mechanisms provide reasonable defence for mote-class outsider attacks. However, cryptography is inefficient in protecting against laptop class and insider attacks. It remains an open problem for additional research and development since the presence of insiders significantly lessens the effectiveness of link layer security mechanisms. This is because an insider is allowed to participate in the network and have complete access to any messages routed through the network and is free to modify, suppress, or eavesdrop on the contents [5].

What makes it even easier for attackers is the fact that most protocols for sensor networks are not designed having security threats in mind. As a consequence, deployments of sensor networks rarely include security protection and little or no effort is usually required from the side of the attacker to perform the attack. So, it is very important to study realistic attacker models and evaluate the practicality and efficiency of certain attacks. The presence of an attacker that can access (and eventually change) the internal state of a sensor node is referred to as node capture in the literature. Most existing routing schemes for sensor networks can be substantially influenced, even if the attacker captures one node or a minute portion of the network [5].

### 3.2 THREATS

There are many possible attacks on wireless sensor network such as selective forwarding, jamming, sinkhole, wormhole, Sybil and hello flood attacks. Sinkhole attack is among the most destructive routing attacks for these networks [4]. The possible vulnerabilities in wireless sensor networks [11] are listed in following table:

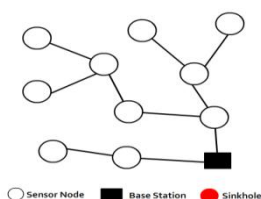
Attack category/features	Type	Damage level	Ease of identity	Attacker presence
Based on access type	Active attacker	High	Easy	Explicit
	Passive attacker	Low	Hard	Implicit
Based on attacker location	External (Outsider)	Low	Medium	Implicit
	Internal (Insider)	High	Hard	Implicit
Based on attacking device	Mote-class attacker	Low	Hard	Implicit
	Laptop-class attacker	High	Easy	Explicit
Based on attack function	Secrecy	High	Hard	Implicit
	Availability	High	Hard	Both
	Stealthy	High	Hard	Implicit

**4. SINKHOLE ATTACK**

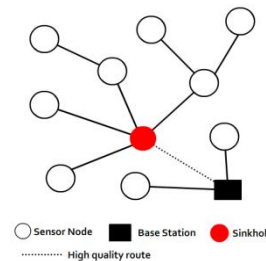
The sinkhole attack is an attack that prevents the base station from obtaining complete and correct sensing data, thus forming a serious threat to higher-layer applications. In a Sinkhole attack, a compromised node advertises attractive and unfaithful routing information. It tries to draw all or as much traffic as possible from itself. As a result, the adversary manages to attract all traffic that is destined to the base station. By taking part in the routing process, sinkhole node can then launch more severe attacks, like selective forwarding, modifying or even dropping the packets coming through [5]. Sinkhole attack is among the most destructive routing attacks for these networks [4].

A sinkhole attack forms a serious threat to sensor networks, particularly considering that the sensor nodes are often deployed in open areas and of weak computation and battery power. The sinkhole node attracts surrounding nodes with unfaithful routing information, and then it alters the data passing through it and performs other operations like selective forwarding [7].

The effect of sinkhole in data flow within WSN is shown in below given figures:



**Figure 1. Dataflow in absence of sinkhole attack**



**Figure 2. Dataflow in presence of sinkhole attack**

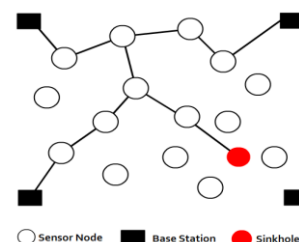
In sinkhole attack, attacker location can be both insider and outsider attacker. Also, mote class and laptop class both can be used as attacking device. Many types of effects of sinkhole attack are listed in [11]. These effects include Luring and to attract almost all the traffic, Triggering other attacks such as eavesdropping, trivial selective forwarding, blackhole and wormhole, Usurp the base station's position, Message modification, Information fabrication and packet dropping, Suppressed messages in a certain area, Routing information modification/fake, and Resource exhaustion [11].

Sinkhole attack is one type attack on routing. Sinkholes are difficult to defend against in protocols where routes are established on the basis of information that is hard to verify, for example, reliability or energy measurements [2]. Several sinkhole detection mechanisms like Data Consistency & Network Flow Information Approach, Hop Count Monitoring Scheme, RSSI Based Scheme, Monitoring node's CPU usage, Mobile Agent Based Approach, Using Message Digest Algorithm are proposed in [4]. Several detection methods like false routing information detection, cooperating neighbouring nodes to each other, Tree structure and verify by tree, verify by Visual Geographical Map are listed in [11].

**5. MULTIPLE BASESTATIONS**

Given that in a WSN, a BS is a laptop class device, the idea of deploying multiple BSs is inexpensive. Use of multiple base stations have been proposed in the literature to handle the flow of large amounts of heterogeneous data from the network and several optimization techniques have been designed for query allocation and base station placement [6], [8], [9].

The mechanism is proposed in [9] that use the placement of multiple BSs to improve the likelihood of packets from the SNs reaching at least one BS in the network, thus ensuring high packet delivery success [9]. The data delivery to all base station is triggered only when mobile agent finds any sinkhole node. The successful data delivery using multiple base stations is shown in below given figure:



**Figure 3. Successful data delivery using multiple basestations**

Other advantages of deploying multiple base stations are as follows [14]:

- 1) Shorten the distance between sensors and BSs to cut down the amount of energy consumption on data transmission
- 2) Expand the network connectivity to improve communication coverage
- 3) Increase data rate and reduce message delay of the network
- 4) Provide backup routes and sinks for better fault tolerance

## 6. MOBILE AGENT

Mobile agent is a software program which is self-controlling and it moves from node to node and checks the presence of sinkhole nodes in the network. Routing through multiple base stations algorithm is only activated when there is a chance of sinkhole attack on the network [8]. The technique of using mobile agent is energy efficient, fast, lightweight and reduces message complexity. An effective solution is proposed that uses multiple base stations to improve the delivery of the packets from the sensor nodes reaching at least one base station in the network, thus ensuring high packet delivery success [8]. The primary goal of mobile agent is to detect the compromised nodes. This is done by giving information of one node to its neighbouring nodes in the network [6]. Application of mobile agent computing model in WSN carries many advantages which are as follows [6]:

- 1) Decrease in energy consumption: Instead of data to be processed, agent is transmitted through network which can dramatically decrease quantity of data transmitted.
- 2) Scalability: System performance without direct relationship with network scale is supportive of balanced load.
- 3) Reliability: It means the capability of overcoming the influence by unreliable network links through reaching the nodes accessed at time of establishing network links and Returning result after link recovered.
- 4) Gradual computing accuracy: With the migration of mobile agent in network, computing result is required to become a gradually accurate. Once the requirement is met, mobile agent can return half-way with effect of energy saving.

The scheme to defend against sinkhole attacks using mobile agents is proposed in [4]. Mobile agent is a program segment which is self controlling. They navigate from node to node not only transmitting data but also doing computation. A routing algorithm with multiple constraints is proposed based on mobile agents. It uses mobile agents to collect information of all mobile sensor nodes to make every node aware of the entire network so that a valid node will not listen to the cheating information from malicious or compromised node which leads to sinkhole attack. It does not need any encryption or decryption mechanism to detect the sinkhole attack. This mechanism does not require more

energy than normal routing protocols [4].

Each node has an information cache that agents can update with more recent values. Nodes access this shared cache whenever they require information about the network [1]. To protect the Mobile agent Dummy data is stored in the data base of the agent. It is not modified while the agent performs its functions. If dummy data is not modified after the agent's returns, then one can have confidence that legitimate data also has not been corrupted [1].

## 7. REFERENCES

- [1] D.Sheela, Naveen kumar. C, and Dr. G.Mahadevan, "A Non Cryptographic Method Of Sink Hole Attack Detection In Wireless Sensor Networks", ICRTIT, 2011.
- [2] Walteneus Dargie, and Christian Poellabauer, "Fundamentals Of Wireless Sensor Networks : Theory And Practice", John Wiley & Sons Ltd, United Kingdom.
- [3] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey", Computer Networks, vol. 38, 2002, pp.393-422.
- [4] Vinay Soni, Pratik Modi, and Vishvash Chaudhri, "Detecting Sinkhole Attack in Wireless Sensor Network", IJAEM, Volume 2, Issue 2, February 2013.
- [5] Ioannis Krontiris, Thanassis Giannetsos, and Tassos Dimitriou, "Launching a Sinkhole Attack in Wireless Sensor Networks; the Intruder Side", WiMob, 2008, pp.526-531.
- [6] Sheela.D, Srividhya.V.R, Asma Begam, Anjali and Chidanand G.M., "Detecting Black Hole Attacks in Wireless Sensor Networks using Mobile Agent", ICAIES, July 15-16, 2012, Singapore.
- [7] Edith C.H. Ngai, Jiangchuan Liu, and Michael R. Lyu, "An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks", Computer Communications, vol. 30, 2007, pp. 2353-2364.
- [8] Nitesh Gondwal, and Chander Diwaker, "Detecting Blackhole Attack In Wsn By Check Agent Using Multiple Base Stations", AIJRSTEM, 3(2), June-August, 2013, pp. 149-152.
- [9] Satyajayant Misra, Kabi Bhattarai, and Guoliang Xue, "BAMBi: Blackhole Attacks Mitigation with Multiple Base Stations in Wireless Sensor Networks", IEEE ICC, Kyoto, 2011, pp.1-5.
- [10] Zdravko Karakehayov, "Using REWARD to detect team black-hole attacks in wireless sensor networks", Real-World Wireless Sensor Networks, June 20-21, 2005.
- [11] Dr. Shahriar Mohammadi, and Hossein Jadidoleslami, "A Comparison Of Link Layer Attacks On Wireless Sensor Networks", GRAPH-HOC, Vol.3, No.1, March 2011.
- [12] Miroslaw Kutylowski, Jacek Cichon, and Przemyslaw Kubiak, "Algorithmic Aspects of Wireless Sensor Networks", Third International Workshop, ALGOSENSORS 2007, Wroclaw, Poland, July 14, 2007.
- [13] Al-Sakib Khan Pathan, Hyung-Woo Lee, and Choong Seon Hong, "Security in Wireless Sensor Networks: Issues and Challenges", ICACT, Feb. 20-22, 2006.
- [14] Yunyue Lin, QishiWu, Xiaoshan Cai, Xiaojiang Du, and

Ki-Hyeon Kwon, "On Deployment of Multiple Base Stations for Energy-Efficient Communication in Wireless

Sensor Networks", IJDSN, Volume 2010, Article ID 563156.